IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 11, Issue 6, November-December 2024

Impact Factor: 7.394

www.ijarety.in editor.ijarety@gmail.com

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106029

A Medical Image Encryption Data Sharing

E.Raju[1], Medisetty Shivani[2], Vislavath Shirisha[3], Gantekampu Sai Nikhil[4]

Assistant Professor, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India[1]

Student, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India[2,3,4]

ABSTRACT: Important requirements, including confidentiality, validity, and integrity, must be met before medical data can be transmitted and stored via cloud-based services. For the safety of medical images, this research suggests a novel hybrid encryption/decryption system that can be used in the healthcare industry. This system investigates novel data-driven perturbation methods. The suggested system's behaviors are examined using the various tests and methodologies that have been put forth. Furthermore, testing with a variety of test photos revealed that the suggested cipher text is quick, highly effective, resilient, and protects medical images, and it has a good ability to endure.

KEYWORDS: Hybrid Encryption, Medical Image Security, Cloud-Based Services, Data Perturbation Methods, Confidentiality and Integrity

I. INTRODUCTION

The security of private medical information is crucial in today's quickly changing communication environment, especially as cloud-based Internet-of-Health Systems (IoHS) become more popular. Because these systems communicate and store medical images and personal data in many locations, they are susceptible to illegal access. This data has been secured using cryptographic algorithms, including more conventional techniques like DES and AES, although their effectiveness and resilience to attacks have been limited. These issues have led to the development of sophisticated encryption systems including bit-level permutation, DNA-based schemes, and one-time key methods. Unfortunately, these approaches are frequently rigid, which leads to the investigation of chaotic systems, which are characterized by their robustness and unpredictability. First, one-dimensional (1D) chaotic maps were employed, but they had flaws due to their small parameter set. In recent years, high-dimensional chaotic systems have been

II. OBJECTIVE

Each of the data security options has pros, cons, and areas of use. The primary factors used for evaluation and selection include security, resistance to assaults, computing cost, time complexity, and dynamical behavior. Due to the cloud storage of patient data in IoHS, it is secure and accessible from various locations. In order to secure medical data in a secure e-healthcare system, the work presented in this paper suggests an enhanced encryption technique. The primary goal is to create an easy-to-use data encryption method with minimal key sensitivity, residual consistency, and high data quality.

III. LITERATURE SURVEY

M.Elhoseny(2021) The development of the Internet of Things (IoT) is predicted to change the healthcare industry and might lead to the rise of the Internet of Medical Things. The IoT revolution is surpassing the presentday human services with promising mechanical, financial, and social prospects. This paper investigated the security of medical images in IoT by utilizing an innovative cryptographic model with optimization strategies. For the most part, the patient data are stored as a cloud server in the hospital due to which the security is vital. So another framework is required for the secure transmission and effective storage of medical images interleaved with patient information. For increasing the security level of encryption and decryption process, the optimal key will be chosen using hybrid swarm optimization, i.e., grasshopper optimization and particle swarm optimization in elliptic curve cryptography. In view of this method, the medical images are secured in IoT framework. From this execution, the results are compared and contrasted, whereas a diverse encryption algorithm with its optimization methods from the literature is identified with the most extreme peak signal-to-noise ratio values, i.e., 59.45 dB and structural similarity index as 1.

Q.Zhag(2020) With the rapid development of network and communication technology, digital image communication has become an important way of information transmission. Therefore, much more attention has been paid to the development of the digital image encryption technology. In this paper, we propose a digital image encryption

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106029

technology based on AES algorithm, and the algorithm implementation in MATLAB. Then, we perform digital image processing, obtain the date that can use the AES encryption algorithm, combine both approaches. Then, the digital image can be encrypted, and the algorithm is realized in MATLAB simulation. Through the comparison of the histogram analysis and the analysis of the key, the result has showed that the method can better realize the effect of encryption and decryption N. B. Slimane (2020) Security of multimedia data becomes an obligation, due the increasing use in smart embedded systems and other domains such as medical industrial and engineering applications. In this paper, we propose a fast, secure and light weight scheme for digital image encryption based on nested chaotic attractors using the Secure Hash Algorithm SHA-1 using only two-diffusion process. The results of security analysis such as statistical tests, differential attacks, key space, key sensitivity, entropy information and the running time are illustrated and compared to recent encryption schemes where the highest security level and speed are improved..

A. Akhavan(2020) Recently an image encryption algorithm based on DNA encoding and the Elliptic Curve Cryptography (ECC) is proposed. This paper aims to investigate the security the DNA-based image encryption algorithm and its resistance against chosen plaintext attack. The results of the analysis demonstrate that security of the algorithm mainly relies on one static shuffling step, with a simple confusion operation. In this study, a practical plain image recovery method is proposed, and it is shown that the images encrypted with the same key could easily be recovered using the suggested cryptanalysis method with as low as two chosen plain images. Also, a strategy to improve the security of the algorithm is presented in this paper.

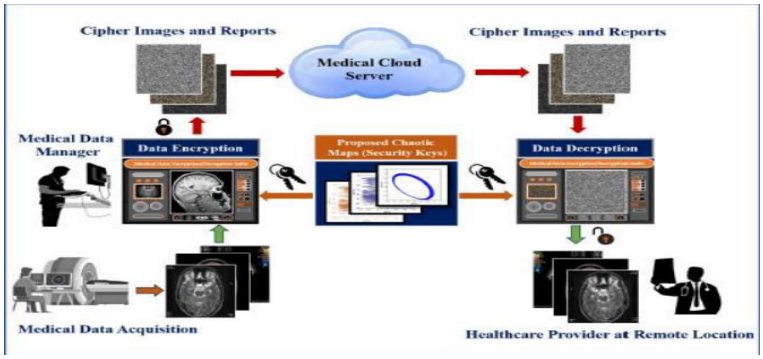
Existing System:
Color-based encryption has been the area of extensive research in recent years. For example, an image encryption algorithm for color images based on the recent. ¬ It achieved a desired effect after two rounds by an exclusive OR (XOR) avalanche operation. Another color-based encryption algorithm that uses a hyper chaotic system and blocks permutation ¬ An encryption system for color image based on the Lorenz system and DNA permutation. It used chaotic pseudo-random sequences depending on plain text images and secret keys.

Existing System Disadvantages:
No Security authentication.
Attackers have accessing directly.
It cannot detect the attackers.

Proposed System
The proposed system incorporates other input parameters besides the plain image and the secret key, to permit controlling the encrypted data values without affecting the secret keys. ¬ Therefore, the suggested algorithm breaks the limitation of those based on keys scheme. ¬ Moreover, our algorithm can encrypt many images securely and speedily using the key. ¬ Experimental results and security review indicate that the proposed could encrypt digital images with high protection and a good ability.

Proposed System Advantage
Stronger authentication
We can give a strong security while sharing an image data.
The overall performance can be improved

System Architecture



| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106029

In this project there are four modules. Each module is doing separate job. Medical cloud server has a get a medical image manager request it has a to be accept. Medical image manager has an upload an image data. It will show a cipher image report it has a sharing a chaotic Map(Keys).If the keys are verified it will get a decryption images. Medical image manager has a send a share keys to health care provider. It will send a key to the patient keys. The Patient has a chaotic key(secret keys) has a sharing a patient. Patient has a get an original image. The other input parameters besides the plain image and the secret key, to permit controlling the encrypted data values without affecting the secret keys.

IV. METHODOLOGIES

We provide an encryption/decryption method for images. The suggested algorithm's central mechanism uses an image process, in which the pixels of an image I that needs to be encrypted are separated into one section (Is, s _ 2). Since we are introducing a key, we select s D 2, so that each image is encoded with one of the alternatives. In general, any number of splits and various (or combinations of) methods can be employed to encode distinct parts of the image. An appropriate set of Is will, at least in part, aid in the regeneration of I, but individual picture sections or splits are thought to communicate no useful information.Despite being an efficient method, contrast and color loss may result in a low-quality restored image. Using keys that have the advantage of having a lower probability of error throughout the encryption and decryption stages, a new and quick method is suggested to partially get around this restriction while maintaining the quality of the recovered image

Modules Name:
1. User Interface Design
2. Medical Cloud Server
3. Medical Image Manager
4. Healthcare Provider
5. Patient

1. User Interface Design
In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.

2. Medical Cloud Server
This is the first module medical cloud server has a register with all details and login. The medical cloud server has a get a medical image manager request. It will have a choice whether it has approved or reject. Afterwords it has an accepted users' details. Medical cloud server has a patient data but it will shows a encrypt image.

3. Medical Image Manager
This is the Second module of this project. In this module medical image manager has a register with all details and login with a user id and password. Medical image manger has an upload an image. Medical image manager has a sending a key to the health care provider. Medical image manger has a key to sharing for health provider.

4.Healthcare Provider
Healthcare provider has a register with a all details and login. Health care provider has a search an image. Healthcare provider has a key response and send to the patient

5. Patient
This is the fourth module of this project. Patient has a register with a details and login. Patient has a keys received from the healthcare provider. Then the patient has a get an original report.

Implementation
A Java implementation for encrypting and sharing medical images securely requires a combination of encryption algorithms, file handling, and possibly networking for sharing. Here's a general plan for building such a solution:

Steps to Implement:
Read Medical Images:
Use libraries like javax.imageio.ImageIO to read image files.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106029

Encrypt the Image:

- Implement AES (Advanced Encryption Standard) or RSA encryption algorithms for image encryption.
- Convert the image to byte arrays for encryption.
- Save the encrypted data as a file or stream it over a network.
- Save or Share the Encrypted Image:
- Save the encrypted data to a secure file.
- Use secure protocols (like HTTPS or SFTP) for sharing.

Decrypt the Image:

- Use the same encryption algorithm for decryption to restore the image.
- User Authentication (Optional):
- Ensure only authorized users can access the encryption or decryption processes by implementing user authentication mechanisms.

Error Handling:

Handle exceptions, such as file not found or encryption errors.

Features of the Code:

- Uses AES encryption for secure data handling.
- Reads and writes files efficiently.
- Saves encryption key securely using Base64 (can be enhanced to store in a secure keystore).
- Can be extended to handle larger images or network sharing.

V. ALGORITHM USED

Existing Algorithm

Step-Wise Grey-Scale Image Encryption Scheme A step-by-step demonstration of the encryption/decryption processes using a chest CT scan. The various processing steps for the application of both encryption stage to obtain the encrypted data . Decryption steps are carried out for splitting the diffused encrypted image; inverting diffusion process for each half using the same keys; inverting the permutation using the similar keys used in encryption process; combing the two halves of the decrypted image to attain the original image. This can only be achieved by using the right secret keys the data has a leaks. We cannot control the attackers. Image has splits the data and keys will cannot detects the attacker. Attacker has directly accessed an image sharing

Proposed Algorithm

AES Based cipher text image We propose image encryption/ decryption scheme. The core of the proposed algorithm employs an image process, where the pixels of a given image I to be encrypted are divided into one portions (Is, s _ 2). Since we introduce key, we choose s D 2, such that each image is encoded using one of the proposed. Generally any number of splits can be used and different (or combinations) can be used for encoding different image portions. The idea behind such process is that individual image portions/splits convey no valuable information, while in the same time an adequate set Is will, at least partially, help to regenerate I . Although being an effective approach, the recovered image may suffer poor quality due to contrast and colors loss. To partially overcome such limitation, a new and fast scheme is proposed utilizing keys that have the advantage of less error chance in encryption/ decryption stages, thus can maintain the quality of the recovered image.

Aes-Based Ciphertext Image Algorithm

Input Image: Read the image file to be encrypted. 2. Key Generation: Generate a secret key for AES encryption. 3. Image Conversion: Convert the image data into a byte array. 4. AES Encryption: Encrypt the byte array using AES. 5. Store/Transmit Ciphertext: Save the encrypted image data (ciphertext) to a file or transmit it securely. 6. Decryption Process: To retrieve the original image, reverse the process using the same key.

Experimental Results

These pages demonstrate the main features and functionalities of the medical cloud server project, including login, dashboard, medical image manager, healthcare provider, and patient pages.

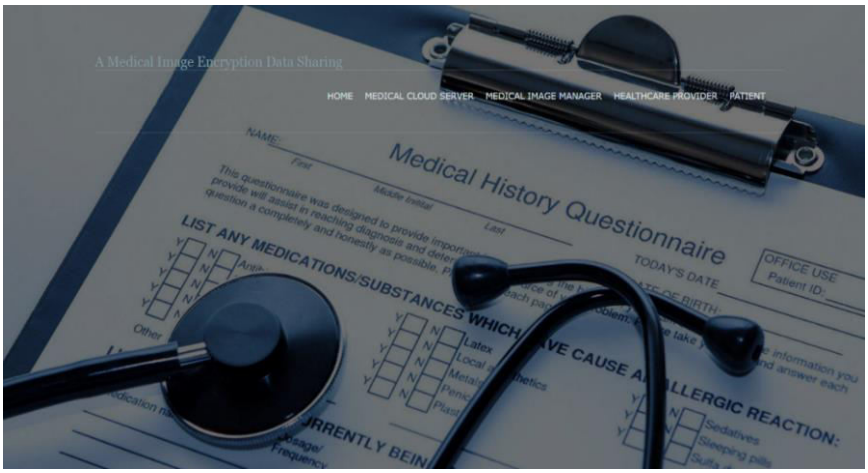
International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

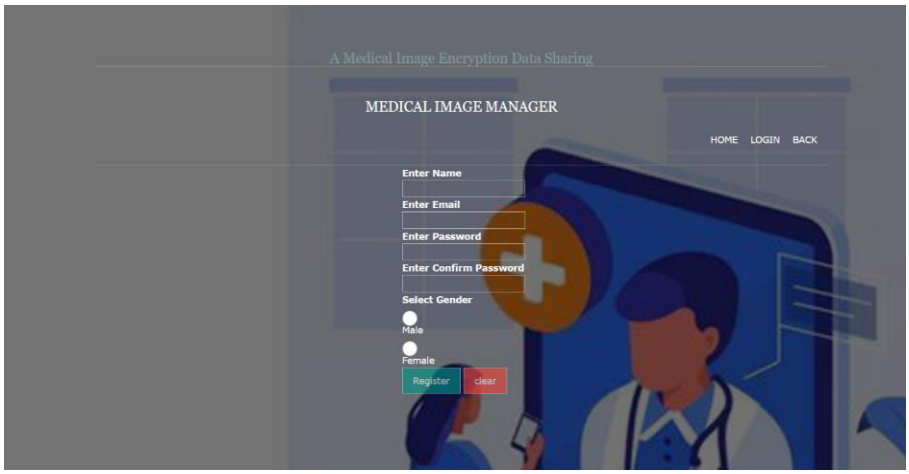
|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106029

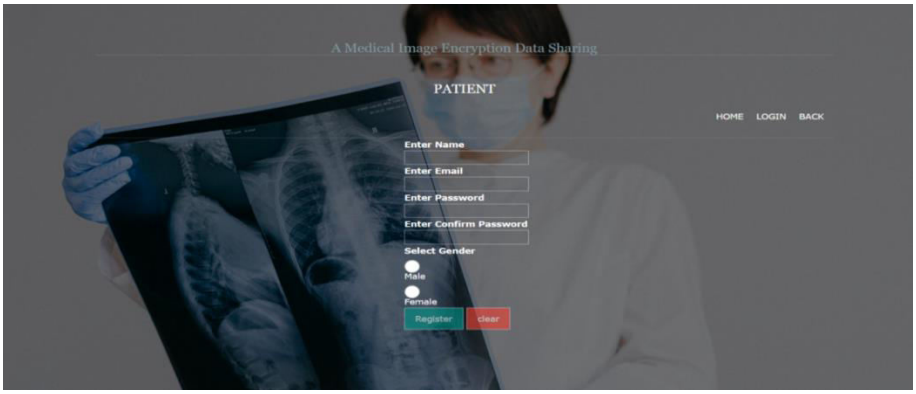
Interface Page



Registration Pages



Medical Image Manager Registration Page



Patient Registration Page

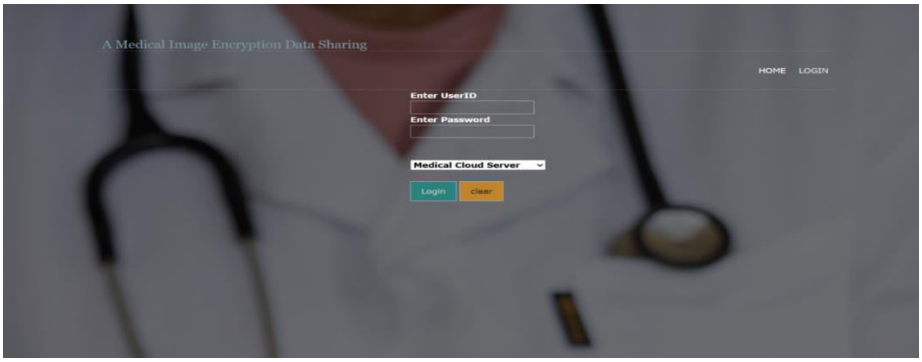
Login Pages

International Journal of Advanced Research in Education and TechnologY(IJARETY)

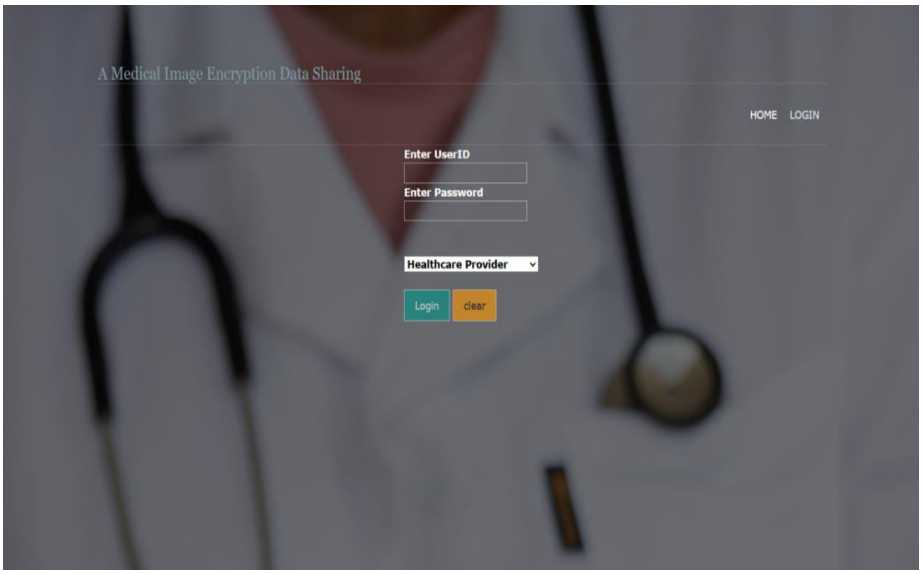
| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

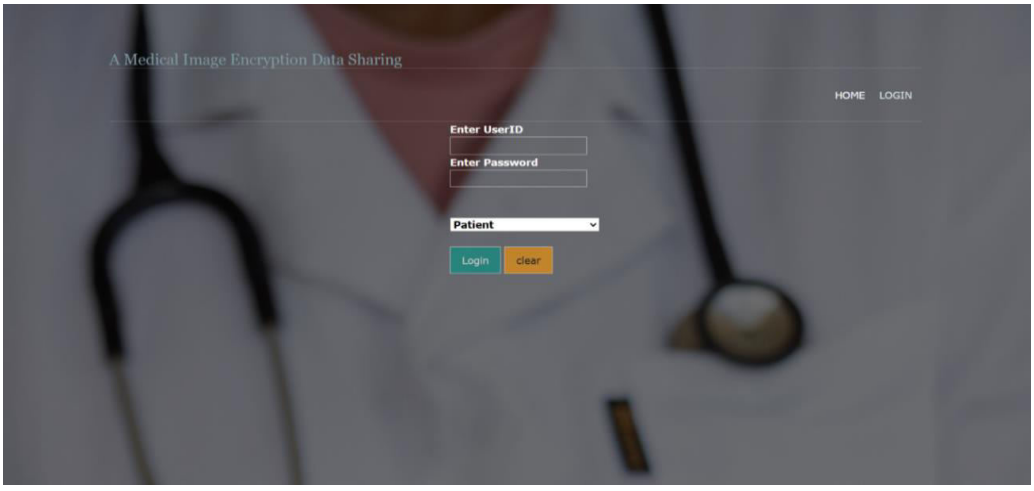
DOI:10.15680/IJARETY.2024.1106029



Cloud Server Login Page



Healthcare Provider Login Page



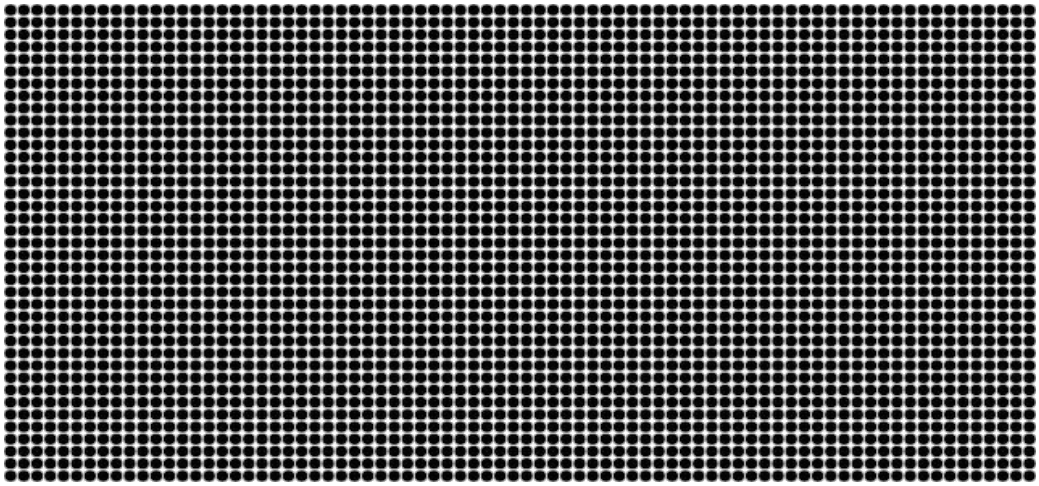
Patient Login Page

International Journal of Advanced Research in Education and TechnologY(IJARETY)

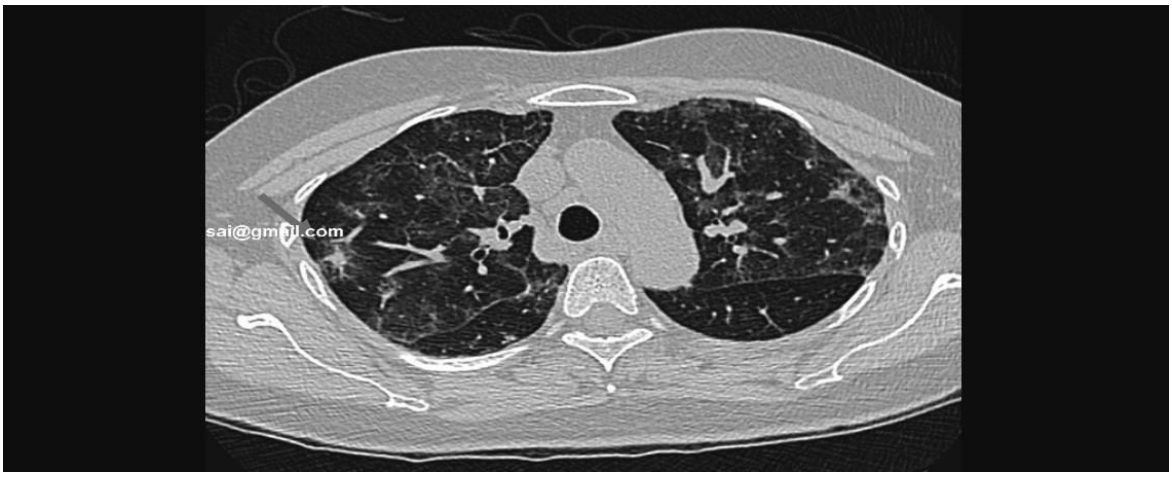
| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106029



Encrypted Image



Decrypted Image

VI. CONCLUSION

This paper has introduced a novel and robust medical image encryption scheme that can integrated in cloud-based internet-of-heath systems (IoHS). The proposed pipeline introduced two novel chaotic maps, which demonstrated strong and effective chaotic behaviors, unpredictability, and extreme sensitive to initial seeds. Dynamic analysis and validation using bifurcation diagram and showed that the proposed maps are hyperchaotic overall with high complexity and high sensitivity. Moreover, the proposed pipeline scheme (1) consists of a two-run confusion-diffusion architecture, and (2) incorporates other input parameters besides the plain image and the secret key unlike those encryption algorithms based on one-time keys. The latter has the advantage that it permits controlling the encrypted data values without affecting the secret keys. Thus, our system breaks the limitation of those based on one-time keys and possess multiple advantage, including improved encryption quality, performance, and robustness; and also secure and speed encryption of many images using the same key. This has been documented using various experiments and various test medical images. Additional companion with state-of-the art encryption scheme using benchmark images (both color and greyscale) highlighted the high effectiveness and robustness of the proposed scheme to prevent many existing cryptography attacks and cryptanalysis techniques. It is worth mentioning that the proposed pipeline is general and can be applied for any multimedia encryption application, including nonmedical ones

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106029

VII. FUTURE ENHANCEMENT

In the future enhancement in our project has a medical image manager has a takes a permission with a medical cloud server. Medical cloud server has a accept the request then only image manager has an upload an image and share with the patient. Key sensitivity is another important analysis procedure that evaluates the characteristics of chaotic coding. Ideally, cipher images should be very sensitive to slight changes in their secret keys

REFERENCES

[1] M. Elhoseny, K. Shankar, S. Lakshmanaprabu, A. Maseleno, and N. Arunkumar, ``Hybrid optimization with cryptography encryption for medical image security in Internet of Things," Neural Comput. Appl., vol. 32, pp. 10979_10993, 2018.
[2] S. Madhu and M. A. Hussain, ``Securing medical images by image encryption using key image," Int. J. Comput. Appl., vol. 104, no. 3, pp. 30_34, Oct. 2014.
[3] J. Li and H. Liu, ``Colour image encryption based on advanced encryption standard algorithm with two-dimensional chaotic map," IET Inf. Secur., vol. 7, no. 4, pp. 265_270, Dec. 2013.
[4] Q. Zhang and Q. Ding, ``Digital image encryption based on advanced encryption standard (AES)," in Proc. 5th Int. Conf. Instrum. Meas., Com- put., Commun. Control (IMCCC), Sep. 2015, pp. 1218_1221.
[5] J. Daemen and V. Rijmen, The Design of Rijndael: AES_The Advanced Encryption Standard. Springer-Verlag, 2002, p. 238, doi: 10.1007/978-3- 662-04722-4.
[6] N. B. Slimane, K. Bouallegue, and M. Machhout, ``Nested chaotic image encryption scheme using two-diffusion process and the secure hash algorithm SHA-1," in Proc. 4th Int. Conf. Control Eng. Inf. Technol. (CEIT), Dec. 2016, pp. 1_5.
[7] X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, ``Color image DNA encryption using NCA map-based CML and one-time keys," Signal Process., vol. 148, pp. 272_287, Jul. 2018.
[8] L. Xu, Z. Li, J. Li, and W. Hua, ``A novel bit-level image encryption algorithm based on chaotic maps," Opt. Lasers Eng., vol. 78, pp. 17_25, Mar. 2016.
[9] A. Akhavan, A. Samsudin, and A. Akhshani, ``Cryptanalysis of an image encryption algorithm based on DNA encoding," Opt. Laser Technol., vol. 95, pp. 94_99, Oct. 2017.
[10] Y. Dou, X. Liu, H. Fan, and M. Li, ``Cryptanalysis of a DNA and chaos based image encryption algorithm," Optik, vol. 145, pp. 456_464, Sep. 2017.
[11] S. K. Pujari, G. Bhattacharjee, and S. Bhoi, ``A hybridized model for image encryption through genetic algorithm and DNA sequence," Proc. Comput. Sci., vol. 125, pp. 165_171, Dec. 2018.
[12] H. M. Waseem, S. S. Jamal, I. Hussain, and M. Khan, ``A novel hybrid secure con_dentiality mechanism for medical environment based on Kramer's spin principle," Int. J. Theor. Phys., vol. 60, no. 1, pp. 314_330, 2021.
[13] H. Liu, A. Kadir, and X. Sun, ``Chaos-based fast colour image encryption scheme with true random number keys from environmental noise," IET Image Process., vol. 11, no. 5, pp. 324_332, 2017.
[14] S. Tariq, M. Khan, A. Algha_s, and M. Amin, ``A novel hybrid encryption scheme based on chaotic Lorenz system and logarithmic key generation," Multimedia Tools Appl., vol. 79, no. 31, pp. 23507_23529, 2020.
[15] U. A. Waqas, M. Khan, and S. I. Batool, ``A new watermarking scheme based on Daubechies wavelet and chaotic map for quick response code images," Multimedia Tools Appl., vol. 79, nos. 9_10, pp. 6891_6914, Mar. 2020.
[16] I. Yasser, M. A. Mohamed, A. S. Samra, and F. Khalifa, ``A chaoticbased encryption/decryption framework for secure multimedia communications," Entropy, vol. 22, no. 11, p. 1253, Nov. 2020.
[17] A. Algha_s, N. Munir, and M. Khan, ``An encryption scheme based on chaotic Rabinovich_Fabrikant system and s8 confusion component," Multimedia Tools Appl., vol. 80, no. 5, pp. 7967_7985, Feb. 2021.
[18] A. Algha_s, H. M. Waseem, M. Khan, S. S. Jamal, M. Amin, and S. I. Batool, ``A novel digital contents privacy scheme based on quantum harmonic oscillator and Schrodinger paradox," Wireless Netw., pp. 1_20, May 2020, doi: 10.1007/S11276-020-02363-7.
[19] Kadiri, P., Anusha, P., Prabhu, M., Asuncion, R., Pavan, V. S., & Suman, J. V. (2024, July). Morphed Picture Recognition using Machine Learning Algorithms. In 2024 Second International Conference on Advances in Information Technology (ICAIT) (Vol. 1, pp. 1-6). IEEE.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 7.394

www.ijarety.in editor.ijarety@gmail.com